UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

HOWARD STERN and GARY LOWENTHAL, individually and on behalf of all others similarly situated, Plaintiffs, v. THE HOME DEPOT INCORPORATED, a Delaware corporation, Defendant.	Case No. _____ Jury Trial Demanded

CLASS ACTION COMPLAINT

Plaintiffs identified below, individually and on behalf of all other persons similarly situated, allege the following claims against The Home Depot, Incorporated ("Home Depot" or the "Company"), based upon personal knowledge with respect to themselves and upon information and belief as to all other matters derived from, among other things, investigation of counsel including review of publicly available documents and information.

NATURE AND SUMMARY OF THE ACTION

1. Beginning in April 2014, Home Depot was subjected to what is reported to be the largest known breach of a retail company's computer networks in history,

when computer 'hackers' were able to steal from Home Depot sensitive personal and financial customer data pertaining to customers who used credit or debit cards at Home Depot's U.S. and Canadian stores (herein, the "Data Breach").

2. The Company publicly confirmed the Data Breach on September 8, 2014, stating that it continues to determine the full scope, scale and impact of the breach and has taken aggressive steps to address the malware and protect customer data. On September 18, 2014, the Company reported that the Data Breach affects the account information of 56 million cardholders, and that the hackers' point of entry has been closed off and that the malware has been removed from its systems.

3. As *Bloomberg News* reported on September 4, 2014, the Home Depot Data Breach is among "only the latest in a long-running series of data hacks." The *Bloomberg News* article reported, "Since 2005, more than 300 data breaches in which 100,000 or more records were compromised have been publicly disclosed."

4. By its acts and omissions alleged herein, Home Depot failed to take adequate and reasonable measures to protect its data systems from malware attacks, failed to take available steps to prevent and stop the Data Breach from ever happening, failed to disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard customers' financial account and personal data, and failed to provide timely and adequate notice of the Data Breach so

that customers could have made an informed decision as to whether to shop at Home Depot.

5. The meager consolations that Home Depot has offered to customers, which customers must take affirmative steps to obtain, provide little to no restitution for most of the harm caused to Plaintiffs and the other members of the Class and Sub-Class. Home Depot's consolations include identity theft protection and credit monitoring service. Home Depot reports that customers will not be responsible for any possible fraudulent charges, because either the banks that issued customers' credit or debit cards or Home Depot are responsible for those charges. However, fraudulent charges and other unauthorized activities stemming from the Data Breach may not become apparent for several years and customers may be subjected to fraud despite Home Depot's meager consolations because of limitations of those services. While Home Depot has advised customers to "closely monitor your payment card accounts and report any unusual activity to your issuing bank," security blogger Brian Krebs, of the website blog *http://www. krebsonsecurity.com* reported, "[C]redit monitoring services are of dubious value because although they may alert you when thieves open new lines of credit in your name, those services do not prevent that activity."

6. On September 14, 2014, Brian Krebs reported the repercussions of the Data Breach may include criminals' ability to "quickly and more accurately locate the

Social Security number and date of birth of cardholders using criminal services in the underground that sell this information." The article also reported:

> The card data for sale in the underground that was stolen from Home Depot shoppers allows thieves to create counterfeit copies of debit and credit cards that can be used to purchase merchandise in big box stores. But if the crooks who buy stolen debit cards also are able to change the PIN on those accounts, the fabricated debit cards can then be used to withdraw cash from ATMs.
>
> * * *
>
> Here's the critical part: The card data stolen from Home Depot customers and for sale on the crime shop Rescator[dot]cc includes both the information needed to fabricate counterfeit cards as well as the legitimate cardholder's full name and the city, state and Zip of the Home Depot store from which the card was stolen (presumably by malware on some part of the retailer's network, and probably on each point-of-sale device).
>
> This is especially helpful for fraudsters since most Home Depot transactions are likely to occur in the same or nearby ZIP code as the cardholder. The ZIP code data of the store is important because it allows the bad guys to quickly and more accurately locate the Social Security number and date of birth of cardholders using criminal services in the underground that sell this information.

7. The September 14, 2014 *Krebsonsecurity.com* article also noted that banks are reporting increased ATM debit card fraud in the wake of the Data Breach, including a large West Coast bank that reported more than $300,000 -- within two hours -- in PIN fraud on debit cards that had been recently used at Home Depot.

Plaintiffs and the other members of the Class and Sub-Class would not have used their credit or debit cards to make purchases at Home Depot, and would not have shopped at Home Depot at all during the period of the Data Breach had Home Depot informed them that it lacked adequate computer systems and data security practices to safeguard customers' personal and financial information from theft, and had Home Depot provided them with timely and accurate notice of the Data Breach.

8. Plaintiffs and the other members of the Class and Sub-Class suffered actual injury from having their credit or debit card account and personal information compromised and stolen as a result of the Data Breach.

9. Plaintiffs and the other members of the Class and Sub-Class suffered actual injury and damages in paying money to and purchasing products or services from Home Depot during the period of the Data Breach that they would not have paid had Home Depot told them that it lacked computer systems and data security practices adequate to safeguard customers' personal and financial information and had Home Depot provided timely and accurate notice of the Data Breach.

10. Plaintiffs and the other members of the Class and Sub-Class suffered actual injury in the form of damages to and diminution in the value of their personal and financial information entrusted to Home Depot for the purpose of purchasing its products, which information was compromised in and as a result of the Data Breach.

11. In addition, all of the individual identity information of each Plaintiff and Class and Sub-Class member constitutes the personal property of said individuals and entities, and Home Depot has thereby improperly taken and/or violated the property rights of each Plaintiff and Class and Sub-Class member.

12. Plaintiffs and the other members of the Class and Sub-Class were overcharged for purchases made at Home Depot stores using their credit or debit cards during the period of the Data Breach in that a portion of the purchase price included the costs of Home Depot providing reasonable and adequate safeguards and data security measures to protect customers' financial and personal data, which Home Depot failed to provide, and as a result, Plaintiffs and the other Class and Sub-Class members did not receive what they paid for and were overcharged.

13. Plaintiffs and the other members of the Class and Sub-Class suffered imminent or impending injury arising from the substantially increased risk of future potential fraud, identity theft and misuse posed by their personal information being placed in the hands of criminals who have already misused such information via sale of the personal and financial information on the underground Internet.

14. Home Depot has not reimbursed customers who suffered a loss of use of their account funds or had restrictions placed on their accounts as a result of the Data

Breach for the loss of access to or restrictions placed upon their accounts and the resulting loss of use of their own funds.

15. Accordingly, Plaintiffs seek to remedy these harms and prevent their future occurrence, on behalf of themselves and all similarly situated consumers. Plaintiffs assert claims against Home Depot for violation of state consumer laws, negligence, breach of implied contract, unjust enrichment and bailment. On behalf of themselves and all similarly situated consumers, Plaintiffs seek to recover damages, including actual and statutory damages, and equitable relief, including injunctive relief to prevent a reoccurrence of the Data Breach, restitution, disgorgement and costs and reasonable attorney's fees.

JURISDICTION AND VENUE

16. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d)(2). The amount in controversy exceeds $5,000,000 exclusive of interest and costs. Plaintiffs and Defendant are citizens of different states. There are more than 100 putative Class and Sub-Class members.

17. This Court has jurisdiction over Home Depot because the Company maintains its principal place of business in Georgia, regularly conducts business in Georgia and has sufficient minimum contacts in Georgia. Home Depot intentionally

avails itself of this jurisdiction by marketing and selling products from Georgia to millions of consumers nationwide, including customers in Georgia.

18. Venue is proper in this Court pursuant to 28 U.S.C. §§1301(a)(2), 1391(b)(2), because: (i) Home Depot maintains its principal place of business in this District; (ii) a substantial portion of the transactions, acts, events, and omissions alleged herein occurred in this District; and (iii) Home Depot received substantial compensation in this District by doing business here and engaging in numerous activities that had an effect in this District.

THE PARTIES

19. Plaintiff Howard Stern is a resident of Monmouth County, New Jersey, and used a credit or debit card to purchase goods at Home Depot's store located in Marlboro, New Jersey during the period of the Data Breach. Plaintiff's financial and personal information associated with his credit or debit card was compromised in and as a result of the Data Breach. Plaintiff was harmed by having his financial and personal information compromised. Plaintiffs incurred a charge of approximately $19.46 on May 21, 2014 on his credit card for purchase of merchandise at Home Depot, and a second charge of $29.75 on September 1, 2014, which was a purchase made by Plaintiff on a date when Home Depot is believed to have known of the Data

Breach but while it was still concealed by Home Depot from the public, including Plaintiffs and the members of the Class and Sub-Class.

20. Plaintiff Gary Lowenthal is a resident of Bergen County, New Jersey and used a credit or debit card to purchase goods at Home Depot's store located in Paramus, New Jersey during the period of the Data Breach. Plaintiff's financial and personal information associated with his credit or debit card was compromised in and as a result of the Data Breach. Plaintiff was harmed by having his financial and personal information compromised. Plaintiffs incurred charges of approximately $25.72 on May 4, 2014, and $25.83 on May 24, 2014 on his credit card for merchandise purchased at Home Depot. Plaintiff's personal information associated with his credit or debit card was thereby compromised in and as a result of the Data Breach by exposure to increased risk of potential fraud, identity theft, and misuse of personal information.

21. Plaintiffs and the other members of the putative Class and Sub-Class consist of, respectively, persons in the United States, and in New Jersey, whose credit or debit card information and/or whose personal information was compromised as a result of the Data Breach first disclosed by Home Depot on September 8, 2014.

22. Defendant Home Depot is a Delaware corporation with principal executive offices located at 2455 Paces Ferry Road N.W., Atlanta, Georgia 30339.

Home Depot describes itself as the world's largest home improvement specialty retailer, with more than 2,200 retail stores in the United States (including Puerto Rico and the U.S. Virgin Islands), Canada and Mexico. The Company's stock is traded on the New York Stock Exchange (NYSE: HD), and is included in the Dow Jones Industrial Average and Standard & Poor's 500 Index.

FACTUAL ALLEGATIONS

23. Plaintiffs are long-time customers of Home Depot who used their Credit or debit cards to purchase merchandise at Home Depot's stores during the period of the Data Breach.

24. On several occasions from April of 2014 to the present, including during the time that Home Depot's data systems were breached by hackers, Plaintiffs purchased goods at the Home Depot stores as set forth in paragraphs 20 and 21 herein, including using a credit card for such purchases. At all material times, Plaintiffs relied upon the security protections of Home Depot's data network to assure that their personal and financial information contained on his credit cards would remain secure and would not be disclosed to third parties.

25. If Plaintiffs had known that Home Depot would not maintain their personal and financial information in a secure manner, they would not have purchased goods at Home Depot using credit cards or would not have purchased them at all.

26. As part of its normal business practices, Home Depot routinely collects its customers' personal and financial information, including payment card account numbers, expiration dates, and security codes. Home Depot assures its customers that it will protect this sensitive private information. The Company's Privacy and Security Statement (the "Policy") assures customers that it "values and respects the privacy of its visitors and customers." The Company's website page for Internet orders designated for in-store pick-up states, "At The Home Depot Inc. we know that your privacy is important to you. That's why protecting any personal information such as your name, address, e-mail address or phone number that you provide to us is of the utmost importance to The Home Depot, Inc. and its subsidiaries, divisions, affiliates, brands and other The Home Depot companies. Please read our Privacy Policy and Security Statement which is designed to help you understand what information we gather online and what we do with that information." However, as explained below, Home Depot failed to protect its customers' privacy.

27. This action arises out of Home Depot's responsibility for a data breach. In violation of their express or implied promise to do so, and contrary to reasonable customer expectations, Home Depot failed to take reasonable steps to maintain their customers' personal and financial information in a secure manner. As a result of Home Depot's lack of appropriate security measures, thieves were able to steal sensitive

personal and financial data from customers who used payment cards at its U.S. and Canadian stores. Many of those customers have had, or are at risk of having, their personal and financial information used to commit fraud and other crimes. For others, constant vigilance will be required to protect themselves from the threat of having their identities stolen.

28. Home Depot failed to ensure that the Company implement and maintain adequate information security policies and procedures prior to connecting their local computer networks to other computer networks. These deficiencies unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft.

29. Home Depot aggravated the damages from the Data Breach by failing to make timely disclosure of the breach. The breach was initially reported publicly in an independent security blog, *http://www.krebsonsecurity.com*, on September 2, 2014. Home Depot reportedly learned of the breach on or about September 1, 2014, reporting that it commenced its investigation on the morning of September 2, immediately "after" it received reports from its banking partners and law enforcement officials that criminals may have hacked its payment data systems. Had Home Depot learned of the breach on the morning of September 2, it would have reported that it commenced its investigation on September 2 immediately *'upon,'* and not *'after,'* receiving reports of

the Data Breach. Therefore, it is believed that the Data Breach was known to Home Depot prior to September 2.

30. Home Depot made no public mention of the Data Breach until September 8, 2014, when it disclosed its investigation of the Data Breach, focused on the period of April 2014 forward, referring to frustration and anxiety caused by the Data Breach. The focus of the investigation on the period of April 2014 to the present indicates that at least 5 months elapsed from the initiation of the breach until the public learned of the breach.

31. The Company also announced on September 8 that it will implement additional security technology by the end of 2014, stating:

> Responding to the increasing threat of cyber-attacks on the retail industry, The Home Depot previously confirmed it will roll out EMV 'Chip and PIN' to all U.S. stores by the end of this year, well in advance of the October 2015 deadline established by the payments industry.

Investigations by Public Officials

32. One day after Home Depot confirmed the Data Breach, on September 9, 2014, the Office of the Attorney General of the State of Connecticut reported that it has launched a joint probe into the data breach in cooperation with attorney generals from at least five other states.

33. On September 10, 2014, the *Columbus Dispatch* reported, "Two U.S. Senators asked the federal government yesterday to investigate a data breach on the payment-card processing systems of Home Depot Inc….", referring to the request as "increased government scrutiny" and "another sign of trouble." The article also reported, "The retailer has yet to say what was stolen, but experts fear that the attackers might have gotten away with more than 40 million payment cards, which would exceed the number taken in last year's unprecedented attack on Target Corp. Home Depot said customers who shopped at its stores as long ago as April were exposed, meaning that the breach extended for more than four months including the busy summer season. That is far longer than the three-week Target breach."

34. According to a September 9, 2014 statement released by Senators Edward Markey of Massachusetts and Richard Blumenthal of Connecticut, "If Home Depot failed to adequately protect customer information, it denied customers the protection that they rightly expect when a business collects such information," and, "[s]uch conduct is potentially unfair and deceptive, and therefore could violate the FTC Act." The Senators also stated, "We are concerned that the retailer's procedures for detecting and stopping operations to steal customer data are inadequate and we call on the Commission to investigate whether Home Depot's security procedures meet a reasonable standard."

35. A September 9, 2014 letter from Senators Blumenthal and Markey to FTC Chair Edith Ramirez, urged the FTC to immediately open an investigation regarding the Data Breach, and described reasons for their request including, in part, the following:

> As reported in the *Los Angeles Times* ("Possible Data Breach at Home Depot Highlights Retailers' Vulnerability', September 4, 2014), Home Depot's cybersecurity system is ranked behind that of other retailers. According to this report, Home Depot takes 1.3 days to clear malware from its system, lagging behind the retail industry average of one day. Online discussions of vulnerabilities on Home Depot's website date back to 2008. These revelations raise serious concerns about Home Depot's responsiveness to potential attacks, particularly in light of other retailers that have recently been targeted by hackers.
>
> As you know, Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45) gives the FTC jurisdiction to investigate companies' privacy and information security policies, procedures, and practices. Given the unprecedented scope and extended duration of Home Depot's data breach, it appears that Home Depot may have failed to employ reasonable and appropriate security measures to protect sensitive personal information.
>
> Furthermore, it is troubling that Home Depot has not yet been able to confirm that it has successfully shut down the data breach. This means that its customers may continue to be at risk of having their personal information stolen. We are concerned that the retailer's procedures for detecting and stopping operations to steal customer data are inadequate and we call on the Commission to

> investigate whether Home Depot's security procedures meet a reasonable standard. If Home Depot failed to adequately protect customer information, it denied customers the protection that they rightly expect when a business collects such information. Such conduct is potentially unfair and deceptive, and therefore could violate the FTC Act.
>
> As the FTC has recognized in the past, data breaches expose consumers to significance and potentially permanent economic harm. Home Depot customers who have their data misused by hackers and thieves risk losing their good credit and in turn, their ability to secure the goods and services they need for their wellbeing and the wellbeing of their families. Even customers whose stolen data is never ultimately misused must live with the fear and uncertainty of knowing their personal information may be circulating for sale on the Internet.
>
> While it is clear that the FTC has the authority to investigate breaches like this one, it is equally clear that the Commission needs additional authority to impose sanctions sufficient to fully punish and deter the conduct that leads to such breaches. The breach at Home Depot highlights how vast and damaging data breaches can be.

36. On September 10, 2014, the Office of U.S. Representative Jan Schakowsky issued a statement critical of Home Depot's failure to notify its customers of the Data Breach, urging Home Depot to "come clean with its customers, take full responsibility for all unauthorized charges, and work closely with law enforcement to prevent all types of fraud that may result from this breach." The statement described the breach as "an attack that went unnoticed by the company for five months," in

which "more than 60 million credit and debit card numbers and associated pieces of personal information were stolen from Home Depot stores." The statement cited particular concern about "recent reports indicating a share increase in fraudulent ATM withdrawals using Home Depot customers' debt card data."

37. On September 11, 2014, U.S. Senator and Chair of the Senate Commerce Committee Jay Rockefeller of West Virginia, and U.S. Senator Claire McCaskill of Missouri sent a letter to Home Depot's chairman and chief executive officer requesting a briefing. The letter, as reported by *Bloomberg News* on September 11, 2014, states, "We ask that Home Depot's information-security officials provide a briefing to committee staff regarding your company's investigation and latest findings on the circumstances that may have permitted unauthorized access to sensitive customer information."

Home Depot's Privacy and Security Policy

38. The provisions of Home Depot's privacy and security policy, as set forth the in Policy, available on the website, at *http://www.homedepot.com/c/Privacy_Security*, are applicable to Home Depot's interactions with customers and visitors, including, but not limited to, as set forth in the "About This Policy" section of the Policy, the Company's stores, among other things:

- Use of [the Company's] websites, including mobile websites

- Visits to [the Company's] stores or attendance at one of [its] events
- Use of applications for mobile phones, tablets or other smart devices
- Phone and email communications
- Social media interactions on our websites and other third party websites like Facebook, YouTube and Twitter
- Viewing [the Company's] online advertisements or emails

39. Home Depot's Policy also includes its security policy, as follows:

> **Security**
>
> When you place orders on our websites, all of your order information, including your credit card number and delivery address, is transmitted through the Internet using Secure Sockets Layer (SSL) technology. SSL technology causes your browser to encrypt your order information before transmitting it to our secure server. SSL technology, an industry standard, is designed to prevent someone other than operators of our websites from capturing and viewing your personal information.
>
> While we use industry standard means to protect our websites and your information, the Internet is not 100% secure. The measures we use are appropriate for the type of information we collect. We cannot promise that your use of our websites or mobile applications will be completely safe. We encourage you to use caution when using the Internet. Online access to your personal information is protected with a password you select. We strongly recommend that you do not share your password.

40. The Security section of Home Depot's Policy contains no express mention in itself of security provisions specifically applicable to in-store purchases. Yet, while the Company's September 8, 2014 acknowledgement of the Data Breach provides that "[t]here is no evidence that the breach has impacted stores in Mexico or customers who shopped online at HomeDepot.com," the "About This Policy" Section of the Policy provides that the Policy is applicable to, among other things, Home Depot's "interactions with [its] customers and visitors, including, but not limited to: . . . "[v]isits to [the Company's] stores." Therefore, the provisions of the Security section of Home Depot's Policy, as well as all other sections of the Policy, are not only applicable to Internet purchases, but are also applicable to in-store purchases. Indeed, several sections of the Policy refer to in-store interactions, including sections/subsections titled: 'About This Policy' ("It applies to our interactions with our customers and our visitors" and, "Visits to our stores or attendance at one of our events"); 'Returns Information' ("When you return an item to our stores or request a refund or exchange…."); 'Demographic Information' ("We may collect information about. . . where you shop."); 'Location Information' ("We use this location data to find our nearest store to you . . . ."); 'How Information is Collected' ("In connection with an online or in-store purchase" and, "If we send you an electronic copy of an in-store receipt."); 'How We Use Information,' subsection 'For security purposes' ("We may

use your information to protect our company, our customers, or our websites. For example, we might use cameras in our stores to track store traffic or our stock."); and, 'How We Use Information,' subsection 'For our marketing' ("For example, if you . . . gave us information in one of our stores.").

41. Home Depot's Policy also describes the information that it collects, as follows, in part:

> **Contact Information**
> We may collect the names and user names of our customers and other visitors. Additionally, we may collect your purchase history, billing and shipping addresses, phone numbers, email addresses, and other digital contact information. We may also collect information that you provide us about others.
>
> **Payment Information**
> When you make a purchase we collect your payment information, including information from your credit or debit card, check, PayPal account or gift card. If you apply for a The Home Depot credit card or a home improvement loan, we might collect information related to your application.
>
> **Returns Information**
> When you return a product to our stores or request a refund or exchange, we may collect information from you and ask you to provide your government issued ID. We use the information we collect from you and capture off of your government issued ID to help prevent fraud. To learn more about our returns policy, click here.
>
> **Demographic Information**

> We may collect information about products or services you like, reviews you submit, or where you shop. We might also collect information like your age or gender.
>
> **Location information**
> If you use our mobile websites or applications, we may collect location data obtained from your mobile devices

42. Home Depot's Policy also describes how it collects information, as follows, in part:

> **We collect information directly from you. The following are a few examples of when we collect information from you:**
>
> - During website or survey registration
> - In connection with an online or in-store purchase
> - If you use an online forum, submit a question or answer to our Product Q&A or provide use with comments or reviews
> - If you upload a photo or other digital content through one of our websites or applications
> - If you register for a loyalty program or apply for a The Home Depot credit card or a home improvement loan
> - If you register for a loyalty program or apply for a The Home Depot credit card or a home improvement loan

- If you participate in a sweepstakes, content, clinic or workshop
- If you rent equipment or vehicles or request warrant or other information
- If you return a product or use a rebate
- If you request we send you an electronic copy of your in-store receipt
- In connection with your interactions with us as a registered user or our websites. For example, when you use the features of our My Account tool like Express Checkout, Address Book, My Lists, My Project Guides, etc.

43. Home Depot's Policy also describes how it uses the information that it collects, as follows, in part:

> **We use the information we collect for our business purposes, including:**
>
> **To respond to your questions and requests. Examples include:**
>
> - Fulfilling orders or providing services
> - Entering you into a sweepstakes or sending you prizes you might have won
> - Registering you for a particular website, loyalty program, or extended warranty service or providing you with information regarding such programs or

services

- Processing a return [….]

- Responding to a product or service review

To improve our products and services.
We make use your information to make website or product and service improvements.

To look at website trends and customer interests.
We might use your information to customize your experience with us. We may also combine information we get from you with other information about you we have received from third parties to assess trends and interests.

For security purposes.
We may use your information to protect our company, our customers, or our websites. For example, we might use cameras in our stores to track store traffic or our stock.

For our marketing.
In certain circumstances, we may send you communications about special The Home Depot promotions or offers. For example, if you have registered on a website and indicated you want to receive this information or if you gave us your information in one of our stores. We may also notify you of new website features or product and service offerings. If permitted, we may also send information about offers from our Affiliates and other companies we think you might find interesting. To manage our communications with you, following the instructions in the Your Privacy Preferences section below.

> **To communicate with you about our relationship.** We may contact you to tell you about changes to this Privacy and Security Statement, the Terms of Use of our websites or mobile applications, or changes to any of our programs in which you might be enrolled. We may also tell you about issues with your orders or if there is a product recall.
>
> **For other uses we may disclose to you.**

Home Depot's Inadequate Security

44. The Data Breach has been confirmed, yet it could have been avoided or largely isolated and mitigated. On September 11, 2014, *Bloomberg News* reported that the malicious software program used in the Data Breach, dubbed FrameworkPOS, is a variety of BlackPOS software. Another variety of BlackPOS was used in another massive retail data breach that occurred in 2013 involving Target Corp. As its name suggests, in both cases variations of BlackPOS software (POS standing for 'point of sale'), were designed to capture credit card numbers when customers swipe their cards at registers. Though variations exist as to how and where the malware installs itself, how it interacts with the operating system and how it hides credit card numbers as they are sent outside the system, both programs are versions of BlackPOS malware. A managing partner at one information security firm reported, "It's the same baseline code that we saw at Target."

45. In the wake of the 2013 Target breach, many banks, credit card companies, and retailers, adopted the use of microchips in credit and debit cards, by installing microchip-enabled checkout terminals to provide greater security than non-microchip-enabled cards. Home Depot, however, did not install microchip-enabled checkout terminals at its stores, despite the massive 2013 Target breach. Home Depot remained vulnerable to such attacks following the 2013 Target breach, and the weakness in its security system continues to be exploitable; its point of sale systems have random access memory that can be "scraped" for credit card data.

46. A *Bloomberg News* article published on September 18, 2014, titled "Home Depot Consultants Urged Security Upgrades Before Hack," reported that according to internal company e-mails and reports, in 2013 Home Depot suffered at least two smaller hacks, after which Home Depot's security contractors "urged the company to strengthen its cyberdefenses by activating a key, unused feature of its security software that the documents say would have added a layer of protection to the retail terminals where customers swipe their cards." The September 18, 2014 article further reported:

> Internal Home Depot documents show the Atlanta-based retailer had chosen to keep an extra security measure deactivated even though it was designed specifically to spot the kind of malicious software that attacks systems'

> endpoint, like the registers that were hit at Target Corp., Michaels Cos., Neiman Marcus Group LLC, and others.
>
> * * *
>
> It's unclear why Home Depot resisted activating the intrusion prevention feature in its software suit, a Symantec Corp. product called Endpoint Protection. The internal documents suggest the program sometimes generated false positives. Two information security managers who previously worked for Home Depot say their supervisor told them to minimize costs and system downtime at the expense of improving security. They and three other former employees, who asked not to be named because they fear retribution, say the information security department has struggled with employee turnover and old software for about three years.
>
> * * *
>
> Security consultants urged Home Depot several times from August 2013 to February 2014 to turn on an Endpoint Protection feature, the internal documents say. According to an Oct. 1, 2013 report prepared for Home Depot by consultant FishNet Security Inc., the retailer left its computers vulnerable by switching off Symantec's Network Threat Protection (NTP) firewall in favor of one packaged with Windows.
>
> 'It is highly advised and recommended the NTP Firewall component be deployed and that Windows Firewall be discontinued,' the report states. For intrusion prevention to work properly, it says, NTP was needed on all Home Depot computers, including register payment terminals. Instead, the company kept the protection off its registers and continued to scan for suspicious activities at the network level, say the internal documents.

47. Instead of protecting customers' financial and personal identifying Information ("PII"), Home Depot opted to enjoy the cost-savings benefits of not

installing microchip-enabled checkout terminals and failed to follow commercially reasonable steps that it should have taken to avoid, or at least lessen, the harm inflicted upon Home Depot's customers upon the Data Breach.

48. On September 19, 2014, *The New York Times* published an article titled "Ex-Employees Say Home Depot Left Data Vulnerable," reporting that "[t]he risks were clear to computer experts inside Home Depot: The home improvement chain, they warned for years, might be easy prey for hackers." As reported in the article:

> [D]espite alarms as far back as 2008, Home Depot was slow to raise its defenses, according to former employees.
>
> * * *
>
> [L]ong before the attack came to light this month, Home Depot's handling of its computer security was a record of missteps, the former employees said. Interviews with former members of the company's cybersecurity team – who spoke on the condition they not be named, because they still work in the industry – suggest the company wa slow to respond to early threats and only belatedly took action.
>
> In recent years, Home Depot relied on outdated software to protect its network and scanned systems that handled customer information irregularly, those people said. Some members of its security team left as managers dismissed their concerns. Others wondered how Home Depot met industry standards for protecting customer data. One went so far as to warn friends to use cash, rather than credit cards, at the company's stores.
>
> * * *

[S]ecurity experts were flabbergasted that Home Depot, one of the world's largest retailers, was caught so flat-footed after the breach at Target, which resulted in the theft of data on more than 40 million cards before the holiday season.

* * *

Several people who have worked in Home Depot's security group in recent years said managers failed to take such threats as seriously as they should have. They said managers relied on outdated Symantec antivirus software from 2007 and did not continuously monitor the network for unusual behavior, such as a strange server talking to its checkout registers.

Also, the company performed vulnerability scans irregularly on the dozen or so computer systems inside its stores and often scanned only a small number of stores. Credit card industry security rules require large retailers like Home Depot to conduct such scans at least once a quarter, using technologies approved by the Payment card Industry Security Standards Council, which develops technical requirements for its members' data security programs. The P.C.I. Council requires that approved, third-party quality security assessors perform routine tests to ensure that merchants are compliant.

And yet, two former employees said, while Home Depot data centers in Austin, Tex., and Atlanta were scanned, more than a dozen systems handling customer information were not assessed and were off limits to much of the security staff. A spokeswoman for the P.C.I. Council in Wakefield, Mass., declined to comment on Home Depot specifically.

'Scanning is the easiest part of compliance,' said Avivah Litan, a cybersecurity analyst at Gartner, a research firm. 'There are a lot of services that do this. They hardly cost

> any money. And they can be run cheaply from the cloud.'
>
> * * *
>
> Several former Home Depot employees said they were not surprised the company had been hacked. They said that over the years, when they sought new software and training, managers came back with the same response: 'We sell hammers.'

Damages Suffered by Plaintiffs and the Other Members of the Class and Sub-Class

49. The injuries to Plaintiffs and the other Members of the Class and Sub-Class include:

(a) unauthorized charges on their debit and credit card accounts;

(b) unauthorized risk of charges on their debit and credit card accounts;

(c) theft of their personal and financial information;

(d) costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

(e) loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their including decreased credit scores and adverse credit notations;

(f) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

(g) the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their credit card and other financial and personal information being placed in the hands of criminals and already misused via the sale of the information on the underground Internet;

(h) damages to and diminution in value of their personal and financial information entrusted to Home Depot for the sole purpose of purchasing products from Home Depot and with the mutual understanding that Home Depot would safeguard the information against theft and not allow access and misuse by others;

(i) money paid for products purchased at Home Depot stores during the period of the Data Breach, in that Plaintiffs and Class and Sub-Class members would not have shopped at Home Depot had it disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' financial and personal

information and had Home Depot provided timely and accurate notice of the Data Breach;

(j) overpayments paid to Home Depot for products purchased during the period of the Data Breach in that a portion of the price for such products paid by Plaintiffs and the other Class and Sub-Class members to Home Depot was for the costs of Home Depot providing reasonable and adequate safeguards and security measures to protect customers' financial and personal data, which Home Depot did not do, and as a result Plaintiffs and the other Class and Sub-Class members did not receive what they paid for and were overcharged by Home Depot; and

(k) continued risk to their financial and personal information, which remains in the possession of Home Depot and which is subject to further breaches so long as Home Depot fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class and Sub-Class members' information in its possession.

CLASS ACTION ALLEGATIONS

50. Plaintiffs bring this class action pursuant to Procedure 23(a) and (b)(3), on behalf of themselves and all others similarly situated, consisting of all persons or entities in the United States, and on behalf of a New Jersey sub-class with respect to Counts 3, 4 and 7 herein, who have had personal or financial data stolen from the Defendant's computer network, and who were damaged thereby (the "Class" or "Sub-

Class" herein). The Class and Sub-Class do not include the Defendant, nor its officers, directors, agents, or employees.

51. The Class and Sub-Class consist of thousands, or possibly millions, of customers of Home Depot located throughout the United States and/or New Jersey. While the exact number of Class and Sub-Class members and the identities of individual Class and Sub-Class members are unknown at this time, and can only be ascertained through appropriate discovery, based on the fact that millions of customer accounts have been affected, the Class and Sub-Class are so numerous that joinder of all members is impracticable.

52. The Defendant's conduct affected all Class and Sub-Class members in exactly the same way. The Defendant's failure to properly safeguard its customers' personal and financial data and in failing to notify customers of the security breach as soon as practical after the breach was discovered is completely uniform among the Class and Sub-Class.

53. Questions of law and fact common to all Class and Sub-Class members predominate over any questions affecting only individual members. Such questions of law and fact common to the Class and Sub-Class include:

a. whether the Defendant acted wrongfully by failing to properly safeguard its customers' financial data;

b. whether Defendants' conduct violated law;

c. whether the Defendant failed to notify Class and Sub-Class members of the security breach as soon as practical after the breach was discovered;

d. whether the Plaintiffs and the other members of the Class and Sub-Class have been damaged, and, if so, what is the appropriate relief; and

e. whether the Defendant breached implied contracts with Class and Sub-Class members by failing to properly safeguard their private and confidential financial and personal data.

54. The Plaintiffs' claims, as described herein, are typical of the claims of all Class and Sub-Class members, as the claims of the Plaintiffs and all Class and Sub-Class members arise from the same set of facts regarding the Defendant's failure to protect Class and Sub-Class members' financial data. The Plaintiffs maintain no interests that are antagonistic to the interests of other Class and Sub-Class members.

55. The Plaintiffs are committed to the vigorous prosecution of this action and have retained competent counsel experienced in the prosecution of class actions of this type. Accordingly, the Plaintiffs are adequate representatives of the Class and Sub-Class and will fairly and adequately protect the interests of the Class and Sub-Class.

56. This class action is a fair and efficient method of adjudicating the claim of the Plaintiffs and the Class and Sub-Class for the following reasons:

a. common questions of law and fact predominate over any question affecting any individual Class or Sub-Class member;

b. the prosecution of separate actions by individual members of the Class and Sub-Class would likely create a risk of inconsistent or varying adjudications with respect to individual members of the Class and Sub-Class thereby establishing incompatible standards of conduct for Defendant or would allow some Class or Sub-Class members' claims to adversely affect other Class or Sub-Class members' ability to protect their interests;

c. this forum is appropriate for litigation of this action since a substantial portion of the transactions, acts, events, and omissions alleged herein occurred in this District;

d. the Plaintiffs anticipate no difficulty in the management of this litigation as a class action; and

e. the Class and Sub-Class are readily definable, and prosecution as a class action will eliminate the possibility of repetitious litigation, while also providing redress for claims that may be too small to support the expense of individual, complex litigation.

57. For these reasons, a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

COUNT I

NEGLIGENCE

58. Plaintiffs incorporate and re-allege the allegations contained in the preceding paragraphs as if fully set forth herein.

59. Home Depot owed a duty to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting personal and financial information in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Home Depot's securities systems to ensure that Plaintiffs' and the other Class and Sub-Class members' personal and financial information in Home Depot's possession were adequately secured and protected. Home Depot further owed a duty to Plaintiffs and the other members of the Class and Sub-Class to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

60. Home Depot owed a duty to Plaintiffs and the other members of the Class and Sub-Class to provide security consistent with industry standards and

requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the personal and financial information of Plaintiffs and the other members of the Class and Sub-Class who used credit or debit cards to make purchases at Home Depot's stores.

61. Home Depot owed a duty of care to Plaintiffs and the other members of the Class and Sub-Class because they were foreseeable and probable victims of any inadequate security practices. Home Depot solicited, gathered, and stored the personal and financial information for its own business purposes and in order to facilitate sales transactions with its customers. Home Depot, in the absence of negligence, should have known that a breach of its systems would cause damages to Plaintiffs and the other members of the Class and Sub-Class and Home Depot had a duty to adequately protect such sensitive financial and personal information.

62. Home Depot owed a duty to timely and accurately disclose to Plaintiffs and the other Class members that their personal and financial information had been or was reasonably believed to have been compromised. Timely disclosure was required, appropriate and necessary so that, among other things, Plaintiffs and the other Class and Sub-Class members could take appropriate measures to avoid unauthorized charges to the credit or debit card accounts, avoid shopping at Home Depot stores, cancel or change usernames and passwords on compromised accounts monitor their

account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services and take other steps to mitigate ameliorate the damages caused by Home Depot's misconduct

63. Plaintiffs and the other members of the Class and Sub-Class entrusted Home Depot with their personal and financial information, including when using their credit or debit cards to make purchases at Home Depot stores, on the premise and with the understanding that Home Depot would safeguard their information, and Home Depot was in a position to protect against the harm suffered by Plaintiffs and the others members of the Class and Sub-Class as a result of the Home Depot data breach.

64. Home Depot's own conduct created a foreseeable risk of harm to Plaintiffs and the other members of the Class and Sub-Class. Home Depot's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent and stop the data breach as set forth herein.

65. Home Depot breached the duties it owed to Plaintiffs and the other members of the Class and Sub-Class by failing to exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the personal and financial information of Plaintiffs the members of the Class and Sub-Class.

66. Home Depot breached the duties it owed to Plaintiffs and the other members of the Class and Sub-Class by failing to properly implement technical systems or security practices that could have prevented the loss of the data at issue.

67. Home Depot breached the duties it owed to Plaintiffs and the other members of the Class and Sub-Class by failing to properly maintain their sensitive personal and financial information in Home Depot's possession which has been or is reasonably believed to have been stolen or compromised.

68. Home Depot, in the absence of negligence, should have known that Plaintiffs and the other members of the Class and Sub-Class were foreseeable victims of a data breach of its systems because of laws and statutes that require Home Depot to reasonably safeguard sensitive payment information.

69. By its acts and omissions described herein, Home Depot unlawfully breached this duty.

70. Plaintiffs and the other members of the Class and Sub-Class were damaged by the Home Depot's breach of this duty.

71. The private financial information and personal information that was compromised by the breach of the Defendant's security included, without limitation, information that was being improperly stored and inadequately safeguarded by the Defendant.

72. The breach of security was a direct and proximate result of the Defendant's failure to use reasonable care to implement and maintain appropriate security procedures reasonably designed to protect the credit and debit card information and other nonpublic information of Plaintiffs and the other members of the Class and Sub-Class. This breach of security and unauthorized access to the private, nonpublic information of Plaintiffs and the other members of the Class and Sub-Class was reasonably foreseeable, particularly in light of the warnings regarding RAM scrapers issued in 2013.

73. The Defendant was in a fiduciary relationship with Plaintiffs and the other members of the Class and Sub-Class by reason of its entrustment with credit and debit card information and other nonpublic information. By reason of this fiduciary relationship, the Defendant had a duty of care to use reasonable means to keep the credit and debit card information and other nonpublic information of the Class and Sub-Class private and secure. The Defendant also had a duty to inform Class and Sub-Class members in a timely manner when their credit and debit card information and other nonpublic information became compromised. The Defendant has unlawfully breached these duties.

74. The compromise of the Plaintiffs' and the other Class and Sub-Class members' nonpublic information, and the resulting burden, fear, anxiety, emotional

distress, loss of time spent seeking to prevent or undo any further harm, and other economic and non-economic damages to the Class and Sub-Class, were the direct and proximate result of Defendant's violation of its duty of care.

75. The Defendant had a duty to timely disclose the data compromise to all customers whose credit and debit card information and other nonpublic information was, or was reasonably believed to have been, accessed by unauthorized persons. Disclosure was required so that, among other things, the affected customers could take appropriate measures to avoid unauthorized charges on their accounts, cancel or change account numbers on the compromised cards, and monitor their account information and credit reports for fraudulent charges. The Defendant breached this duty by failing to notify Plaintiffs and the other Class and Sub-Class members in a timely manner that their information was compromised. The Class and Sub-Class members were harmed by the Defendant's delay because, among other things, fraudulent charges have been made to the Class and Sub-Class members' accounts.

76. The Defendant knew or should have known that its network for processing and storing credit and debit card transactions and related information had security vulnerabilities. The Defendant was negligent in continuing such data processing in light of those vulnerabilities and the sensitivity of the data.

77. As a direct and proximate result of the Defendant's conduct, Plaintiffs and the other members of the Class and Sub-Class suffered damages including, but not limited to, loss of control of their credit card and other personal financial information; monetary loss for fraudulent and/or unauthorized charges incurred on their accounts; fear and apprehension of fraud, loss of money, and identity theft; the burden and cost of closing compromised accounts and opening new accounts; the burden of closely scrutinizing credit card statements for past and future transactions; damage to their credit history; loss of privacy; and other economic damages.

COUNT II

BREACH OF IMPLIED CONTRACT

78. Plaintiffs incorporate and re-allege the allegations contained in the preceding paragraphs as if fully set forth herein.

79. By providing Plaintiffs' and the other Class and Sub-Class members' financial and personal information to Home Depot in order to make purchases at Home Depot stores, Plaintiffs and the other Class and Sub-Class members entered into implied contracts with Home Depot pursuant to which Home Depot agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and the other Class and Sub-Class members that their data had been breached and compromised.

80. Home Depot solicited and invited Plaintiffs and the other members of the Class and Sub-Class to purchase products at Home Depot stores using their credit or debit cards. Plaintiffs and the other members of the Class and Sub-Class accepted Home Depot's offers and used their credit or debit cards to purchase products at Home Depot stores during the period of the Data Breach.

81. Each purchase made at a Home Depot store by Plaintiffs and the other members of the Class and Sub-Class using a credit or debit card was made pursuant to the mutually agreed upon implied contract with Home Depot under which Home Depot agreed to safeguard and protect Plaintiffs' and the other Class and Sub-Class members' personal and financial information, including all information contained in the magnetic strip of Plaintiffs' and the other Class and Sub-Class members' credit or debit cards, and to timely and accurately notify them that such information was compromised and breached.

82. Plaintiffs and the other members of the Class and Sub-Class fully performed their obligations under the implied contracts with Home Depot.

83. Defendant breached the implied contracts it had made with the Plaintiffs and the other members of the Class and Sub-Class by failing to safeguard and protect the personal and financial information of Plaintiffs and the other members of the Class and Sub-Class, and by failing to provide timely and accurate notice to them that their

personal and financial information was compromised in and as a result of the Data Breach.

84. The losses and damages sustained by Plaintiffs and the other Class and Sub-Class members as described herein were the direct and proximate result of the Defendant's breaches of these implied contracts.

COUNT III

VIOLATION OF THE NEW JERSEY BREACH OF SECURITY STATUTE N.J. Stat. Ann. §56:8-163(a), *et seq*

85. Plaintiffs incorporate and re-allege all allegations contained in the preceding paragraphs as if fully set forth herein. This claim is brought by Plaintiffs on their own behalf and on behalf of other similarly situated members of the Sub-Class.

86. Plaintiffs and the other members of the Sub-Class are consumers who used their credit or debit cards to purchase products from Home Depot's stores for personal, family or household purposes.

87. Home Depot engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of goods or services to consumers, including Plaintiffs and the other members of the Sub-Class.

88. Home Depot is engaged in, and its acts and omissions affect, trade and commerce. Home Depot's acts, practices and omissions were done in the course of

Home Depot's business of marketing, offering for sale, and selling goods and services throughout the United States, including in New Jersey.

89. Home Depot's conduct, as alleged in this Complaint, including without limitation Home Depot's failure to maintain adequate computer systems and data security practices to safeguard customers' personal and financial information, Home Depot's failure to disclose the material fact that Home Depot's computer systems and data security practices were inadequate to safeguard customers' personal and financial data from theft, Home Depot's failure to disclose in a timely and accurate manner to Plaintiffs and the other members of the Sub-Class the material fact of the Data Breach and Home Depot's continued acceptance of Plaintiffs' and the other Sub-Class members' credit and debit card payments for purchases at Home Depot after Home Depot knew or in the absence of negligence should have known of the data breach and before it purged its data systems of malware, constitutes unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices.

90. By failing to timely notify customers of the Data Breach, Home Depot violated N.J. Stat. Ann. §56:8-163(a), *et seq.*, which provides:

> (a) Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who

> is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection c. of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible. Any determination shall be documented in writing and retained for five years.
>
> * * *
>
> c(2) The notification required by this section shall be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation and that agency has made a request that the notification be delayed. The notification required by this section shall be made after the law enforcement agency determines that its disclosure will not compromise the investigation and notifies that business or public entity.
>
> * * *
>
> 56:8-166 It shall be an unlawful practice and a violation of P.L. 1960, c.39 (C.56:8-1 et seq.) to willfully, knowingly or recklessly violate sections 10 through 13 of this amendatory and supplementary act.

91. The Home Depot Data Breach constituted a breach of the security system of Home Depot within the meaning of the above New Jersey data breach statute and the data breached was protected and covered by the data breach statute.

92. Home Depot unreasonably delayed informing the public, including Plaintiffs and the members of the Sub-Class, about the Data Breach after Home Depot knew or should have known that the Data Breach had occurred.

93. While the Data Breach began in April 2014, Home Depot did not notify customers of the Data Breach until September 8, 2014.

94. When Home Depot was eventually informed of breach by third parties on or about September 1, 2014, Home Depot took no action to disclose or notify the public of the Data Breach, while the breach continued.

95. Eventually Home Depot disclosed the Data Breach, on September 8, 2014, a full week after it learned of the Data Breach and more than 5 months after it commenced, while attempting to minimize its significance to the public, asserting that "there is no evidence that debit PIN numbers were compromised," and attempting to justify its delay, "We owe it to our customers to alert them that we now have enough evidence to confirm that a breach has indeed occurred."

96. Home Depot failed to disclose the Data Breach to Plaintiffs and the other members of the Sub-Class without unreasonable delay and in the most expedient time possible.

97. Home Depot has provided no indication that any law enforcement agency requested that Home Depot delay notification.

98. Plaintiffs and the other members of the Sub-Class suffered harm directly resulting from Home Depot's failure to provide and the delay in providing notification of the Data Breach with timely and accurate notice as required by law.

99. As a result of said deceptive trade practices, Defendant has directly, foreseeably, and proximately caused damages to Plaintiffs and the other members of the Sub-Class. Had Home Depot provided timely and accurate notice of the Data Breach Plaintiffs and the other members of the Sub-Class would have been able to avoid and/or attempt to ameliorate or mitigate the damages and harm resulting in the unreasonable delay by Home Depot in providing notice. Plaintiffs and the Sub-Class members could have avoided making credit or debit card purchases at Home Depot stores, could have avoided shopping at Home Depot stores at all, and could have contacted their banks to cancel their cards, or could otherwise have tried to avoid the harm caused by Home Depot's delay in providing timely and accurate notice.

COUNT IV

BREACH OF NEW JERSEY CONSUMER FRAUD ACT
(N.J. Stat. Ann. 56:8-1, *et seq.)*

100. Plaintiffs incorporate and re-allege all allegations contained in the preceding paragraphs as if fully set forth herein. This claim is brought by Plaintiffs on their own behalf and on behalf of other similarly situated members of the Sub-Class.

101. Plaintiffs and the other members of the Sub-Class conferred a monetary benefit upon Home Depot in the form of monies paid for the purchase of goods from Home Depot during the period of the Data Breach.

102. Home Depot has knowledge of the benefits conferred directly upon it by Plaintiffs and the other members of the Sub-Class.

103. Under the New Jersey Consumer Fraud Act ("NJCFA" or "Act"), to violate the Act, a person must commit an "unlawful practice" as defined in the legislation. Unlawful practices fall into three general categories: affirmative acts, knowing omissions, and violation of any express regulations.

104. Home Depot's violation of the New Jersey Disclosure of Breach of Security statute violates the NJCFA because it constitutes an unconscionable commercial practice and knowing omission, as well constituting a violation of a regulation (*e.g.*, N.J. Stat. Ann. §56:8-163(a), *et seq.*).

105. As a result of Home Depot's unconscionable commercial practice and violation of a regulation, Plaintiffs and Sub-Class members have suffered an ascertainable loss in that they may have their property utilized in an unauthorized manner; they are forced to obtain credit security subscriptions to monitor the action in their various accounts; and they have suffered damages as set forth hereinabove with great specificity and particularization at Paragraphs 9 through 15.

106. By virtue of the aforestated actions and the Data Breach, as well as Home Depot's unconscionable failure to disclose said breach in a timely fashion, Home Depot, has violated the NJCFA. Accordingly, Plaintiffs and the other Sub-Class members have suffered an ascertainable loss as a result of the unlawful acts complained of in the proceeding paragraphs and are therefore entitled to the relief afforded by N.J.S.A. 56:8-1 *et seq.*, including monetary relief and injunctive.

COUNT V

UNJUST ENRICHMENT

107. Plaintiffs incorporate and re-allege all allegations contained in the preceding paragraphs as if fully set forth herein.

108. Plaintiffs and the other members of the Class and Sub-Class conferred a monetary benefit upon Home Depot in the form of monies paid for the purchase of goods from Home Depot during the period of the Data Breach.

109. Home Depot has knowledge of the benefits conferred directly upon it by Plaintiffs and the other members of the Class and Sub-Class.

110. The monies paid for the purchase of goods by Plaintiffs and the other members of the Class and Sub-Class to Home Depot during the period of the Data Breach were supposed to be used by Home Depot, in part, to pay for the administrative

and other costs of providing reasonable data security and protection to Plaintiffs and the other members of the Class and Sub-Class.

111. Home Depot failed to provide reasonable security, safeguards and protection to the personal and financial information of Plaintiffs and the other members of the Class and Sub-Class and, as a result, Plaintiffs and the other members of the Class and Sub-Class overpaid Home Depot for the goods purchased through use of their credit and debit cards during the period of the Data Breach.

112. Under principles of equity and good conscience, Home Depot should not be permitted to retain the money belonging to Plaintiffs and the other members of the Class and Sub-Class, because Home Depot failed to provide adequate safeguards and security measures to protect Plaintiffs' and the other Class and Sub-Class members' personal and financial information that they paid for but did not receive.

113. As a result of Home Depot's conduct as set forth in this Complaint, Plaintiffs and the other members of the Class and Sub-Class suffered damages and losses as stated above, including monies paid for Home Depot products that Plaintiffs and the other members of the Class and Sub-Class would not have purchased had Home Depot disclosed the material facts that it lacked adequate measures to safeguard customers data and had Home Depot provided timely and accurate notice of the Data

Breach, and including the difference between the price they paid for Home Depot's goods as promised and the actual diminished value of its goods and services.

114. Plaintiffs and the other members of the Class and Sub-Class have conferred directly upon Home Depot an economic benefit in the nature of monies received and profits resulting from sales and unlawful overcharges to the economic detriment of Plaintiffs and the other members of the Class and Sub-Class.

115. The economic benefit, including monies the paid and the overcharges and profits derived by Home Depot and paid by Plaintiffs and the other members of the Class and Sub-Class, is a direct and proximate result of Home Depot's unlawful practices as set forth in this Complaint.

116. The financial benefits derived by Home Depot rightfully belong to Plaintiffs and the other members of the Class and Sub-Class.

117. It would be inequitable under established unjust enrichment principles for Home Depot to be permitted to retain any of the financial benefits, monies, profits and overcharges derived from Home Depot's unlawful conduct as set forth in this Complaint.

118. Home Depot should be compelled to disgorge into a common fund for the benefit of Plaintiffs and the other members of the Class all unlawful or inequitable proceeds received by Home Depot.

119. A constructive trust should be imposed upon all unlawful or inequitable sums received by Home Depot traceable to Plaintiffs and the other members of the Class and Sub-Class.

COUNT VI

BAILMENT

120. Plaintiffs incorporate and re-allege all allegations contained in the preceding paragraphs as if fully set forth herein.

121. Plaintiffs and the other members of the Class and Sub-Class delivered their personal and financial information, including information contained on the magnetic strips of their credit and debit cards, to Home Depot for the exclusive purpose making purchases from Home Depot at Home Depot stores.

122. In delivering their personal and financial information to Home Depot, Plaintiffs and the other members of the Class and Sub-Class intended and understood that Home Depot would adequately safeguard their personal and financial information.

123. Home Depot accepted possession of Plaintiffs' and the other Class and Sub-Class members' personal and financial information for the purpose of accepting payment of goods purchase by Plaintiffs and the other members of the Class and Sub-Class at Home Depot stores.

124. In accepting possession of Plaintiffs' and the other Class and Sub-Class members' personal and financial information, Home Depot understood that Plaintiffs and the other Class and Sub-Class members expected Home Depot to adequately safeguard their personal and financial information. Accordingly a bailment (or deposit) was established for the mutual benefit of the parties.

125. During the bailment (or deposit), Home Depot owed a duty to Plaintiffs and the other members of the Class and Sub-Class to exercise reasonable care, diligence and prudence in protecting their personal and financial information.

126. Home Depot breached its duty of care by failing to take appropriate measures to safeguard Plaintiffs' and the other Class and Sub-Class members' personal and financial information, resulting in the unlawful and unauthorized access to and misuse of Plaintiffs' and the other Class and Sub-Class members' personal and financial information.

127. Home Depot further breached its duty to safeguard Plaintiffs' and the other Class and Sub-Class members' personal and financial information by failing to timely and accurately notify them that their information had been compromised as a result of the Data Breach.

128. Home Depot failed to return purge or delete the personal and financial information of Plaintiffs' and the other Class and Sub-Class members at the conclusion of the bailment (or deposit) and within the time limits allowed by law.

129. As a direct and proximate result of Home Depot's breach of its duty, Plaintiffs and the other members of the Class and Sub-Class suffered consequential damages that were reasonably foreseeable to Home Depot, including but not limited to the damages sought herein.

130. As a direct and proximate result of Home Depot's breach of its duty, the personal and financial information of Plaintiffs' and the other Class and sub-Class members' entrusted to Home Depot during the bailment (or deposit) was damaged and its value diminished.

131. Plaintiffs and the other members of the Class and Sub-Class have no adequate remedy at law.

COUNT VII

(Violation of Truth-in-Consumer Contract, Warranty and Notice Act [TCCWNA], N.J.S.A. 56:12-14)

132. Plaintiff incorporates and re-alleges all allegations contained in the preceding paragraphs as if fully set forth herein. This claim is brought by Plaintiffs on their own behalf and on behalf of other similarly situated members of the Sub-Class.

133. TCCWNA provides in part that:

> "No seller…shall in the course of his business offer to any consumer or prospective consumer or enter into any written contract or give or display any written consumer warranty, notice or sign…***which includes any provision that violates a clearly established right of a consumer or responsibility of a seller***…as established by State or Federal Law at the time the offer is made or the consumer contract is signed or the warranty, notice or sign is given or displayed." (emphasis added)

134. The rights afforded to Plaintiffs and Sub-Class members pursuant to N.J. Stat. Ann. §56:8-163(a), *et seq.*, is a clearly established right which were violated by Defendant's failure to timely notify Plaintiffs and Sub-Class members of the Data Breach. As Defendant's breaches are violative of a clearly established consumer right and/or of the responsibilities of the seller, Home Depot has violated the Truth-in-Consumer Contract, Warranty and Notice Act.

135. The Data Breach was also an unconscionable commercial practice and violation of a regulation under New Jersey Consumer Fraud Act, constituting violations of the New Jersey Consumer Fraud Act and a breach of contract. As Home Depot's acts, omissions and Data Breach were violative of a clearly established consumer right and/or of the responsibilities of the seller, Home Depot has violated the Truth-in-Consumer Contract, Warranty and Notice Act.

136. TCCWNA provides that: "any person who violates the provisions of this

act shall be liable to the aggrieved consumer whom he aggrieved or injured for a civil damages penalty of not less than $100.00 or for actual damages, or both at the election of the consumer, together with reasonable attorney's fees and court costs. The rights, remedies and prohibitions accorded by the provisions of this act are hereby declared to be in addition to and cumulative of any other right, remedy or prohibition accorded by common law, Federal law or statutes of this State.

137. Home Depot has violated TCCWNA and the Plaintiff and Sub-Class members request civil damages penalties of not less than $100.00 per violation and attorney's fees afforded under N.J.S.A. 56:12-14.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, respectfully request the following relief:

a. that this Court certify this action as a Class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3), and appoint the Plaintiffs as Class representatives and their counsel as Class counsel to represent the Class and Sub-Class;

b. that this Court enter judgment in favor of Plaintiffs and the other members of the Class and Sub-Class, and against the Defendant under the legal theories alleged herein;

c. that this Court award Plaintiffs and the other members of the Class

and Sub-Class appropriate relief, including actual and statutory damages, restitution and disgorgement;

d. that this Court award attorney's fees, expenses, and costs of this suit;

e. that this Court award the Plaintiffs and the other members of the Class and Sub-Class pre-judgment and post-judgment interest at the maximum rate allowable by law;

f. that the Court award the Plaintiffs and the other members of the Class and Sub-Class equitable, injunctive and declaratory relief as may be appropriate under applicable laws. Plaintiffs on behalf of the other members of the Class and Sub-Class seek appropriate injunctive relief designed to ensure against the recurrence of a data breach by adopting and implementing reasonable data security practices to safeguard customers' financial and personal information, by an Order requiring Home Depot to implement reasonable data security enhancements as they become available, including regular scanning of its data systems for beaches and implementation of EMV microchip technology at Home Depot's point-of-purchase registers.

g. that this Court enter such additional orders or judgment as may be

necessary to prevent the Data Breach from recurring and to restore any interest or any money or property which may have been acquired by means of violations set forth in this Complaint;

h. that this Court award such other and further relief as it may deem just and appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs, individually and on behalf of all others similarly situated, demand a trial by jury on all issues so triable.

DATED: September 22, 2014

Respectfully submitted,

/s/ James M. Evangelista
James M. Evangelista
Georgia Bar No. 707807
Jeffrey R. Harris
Georgia Bar No. 330315
Darren W. Penn
Georgia Bar No. 571322
HARRIS PENN LOWRY LLP
400 Colony Square, Suite 900
1201 Peachtree Street, NE
Atlanta, GA 30361
404.961.7650 (*telephone*)
404.961-7651 (*facsimile*)

Howard Longman
Jason D'Agnenica

STULL, STULL & BRODY
6 East 45th Street
New York, NY 10017
(212) 687-7230 (*telephone*)
(212) 490-2022 (*facsimile*)

Gary S. Graifman
KANTROWITZ, GOLDHAMER & GRAIFMAN, P.C.
210 Summit Avenue
Montvale, New Jersey 07645
Tel: (201) 391-7000 (*telephone*)
Fax: (201) 307-1086 (*facsimile*)

Counsel for Plaintiffs